UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 09-10243-MLW
	)	
RYAN HARRIS	)	

DEFENDANT'S REPLY TO COURT'S PRETRIAL ORDER

Defendant, Ryan Harris, submits this memorandum in response to the Court's Pretrial Order 1) to set out requested pretrial instructions and rulings of law; 2) to respond to the Court's Order of December 14, 2011; and 3) to request rulings on motions in limine regarding evidentiary issues.

I. OVERVIEW

As Harris explained in his motion to dismiss, this is a case of first impression that tests the limits of criminal liability. Among other factfinding, the jury will be asked to evaluate whether the pure act of distribution or sale of the product, which the government contends is "inherently susceptible" to misuse, can support a wire fraud conviction. The law ordinarily protects commercial activity, including the sale of goods that are known to be dangerous (such as cigarettes and hollow point bullets) unless those goods are legally restricted (such as cocaine or heroin). This case, however, attempts to impose liability, unprecedented even in the civil arena, on the manufacturer of a legal product.

Distribution of hacking tools is widespread, and such tools are not legally prohibited or restricted. See Top 15 Security/Hacking Tools & Utilities, at http://www.darknet.org.uk/2006/04/top-15-securityhacking-tools-utilities/ (Apr. 17, 2006).

Examples include Nmap, Nessus, John the Ripper, Cain and Abel, SuperScan, p0f, and Winzapper, as well as vulnerability scanner/injector Metasploit. See SecTools.Org: Top 125 Network Security Tools, at http://sectools.org/ (last visited Jan. 24, 2012. Some hacking tools are sniffers, devices that permit the capture of data transmitted across networks. Id. at http://sectools.org/tag/sniffers/. In an interview, the founder of the Metasploit Project, which publishes the tool called the Swiss Army knife of hackers, was asked:

> **Some people claim that your project helps the bad guys do bad things . . .**
> **H.D. Moore**: The Metasploit Framework strives to be an open platform that anyone can use for just about any purpose. Our users include security researchers, academics, system administrators, penetration testers, software vendors, and yes, even script kiddies. The value provided by making the software available to everyone outweighs any damage caused by the minority that uses the software to illegally access computer systems. The Framework isn't all that great as a script kiddie tool, since the amount of disk space and library requirements make it cumbersome to transfer between compromised hosts.
>
> ***
>
> **Do you see a day when exploits and/or frameworks like Metasploit are regulated by the law?**
> **H.D. Moore**: Exploits are already regulated by law in some countries (France and Germany). I do what I can to prevent this from coming to pass in the United States, by donating to the EFF and trying to make a strong case for the usefulness of exploit code. In the US, exploit regulation would kill research and lead to a degrading state of security for all US companies. Vendors patch because exploits are available, without "above ground" exploits that anyone can access, there is no motivation to patch flaws.

Federico Biancuzzi, Day Dawns for Metasploit 3.0: H.D. Moore unveils the latest release, The Register, Apr. 2, 2007, at http://www.theregister.co.uk/2007/04/02/metasploit_3/print.html.

Notwithstanding wide-ranging commercial practices and a longstanding legal consensus that the sale of an unregulated object alone is not illegal, and that sale alone is not a conspiracy, the government offers instructions stating that the inherent susceptibility of a product to illegal use can support a conviction. It also wishes to argue that the sale of sniffers (and their use in

obtaining MAC addresses and configuration files) is criminal, citing no legal support.

Moreover, it wishes to argue that Harris's website had a forum which permitted the exchange of ideas and information, some of which pertained to obtaining free internet service. Despite the statutory protection for forum operators against claims based on forum content and constitutional concerns that imposing a duty on forum moderators to monitor forum content could infringe the First Amendment rights of participants, the government claims that this forum and its content prove (1) that Harris knew that people were using TCNISO products to obtain free internet, and (2) that Harris is responsible for that content such that it can link Harris in a hub-and-spoke conspiracy with all product users at all times. It is impossible to escape the irony that ISPs (the alleged victims in this case) are currently conducting a massive campaign to urge Congress to reject SOPA (Stop Online Piracy Act) because the ISPs believe they should not be responsible for monitoring the content of the websites they transmit. Services such as eBay, Craigslist, Etsy, AirBnB, Tumblr, Twitter, YouTube, WordPress, and Soundcloud are also vigorously contesting the notion that they are responsible for the content of users' posts on their sites. Yet here the government wishes to offer the speech of unknown forum participants as the plus factor that moves these facts from buyer-seller to conspiracy, in other words, as substantive proof that Harris has committed a crime.

II. REQUESTED PRELIMINARY INSTRUCTIONS

Given the novelty of this case, Harris requests the following preliminary instructions to orient the jury before the trial begins. Harris also proposes these instructions for the end of trial.

1. There is no law prohibiting the modification or sale of altered modems, even altered modems that an individual could use to get free or enhanced internet

access. Proof that Harris made and sold altered modems does not suffice to establish guilt.[1]

2. Product capability alone does not establish culpability.[2] Proof that individuals used altered modems to obtain free internet access does not, alone, establish Harris's guilt.[3]

---

[1] This instruction derives from United States v. Falcone, 311 U.S. 205 (1940) and Direct Sales Co. v. United States, 319 U.S. 703, 710-11 (1943). In Direct Sales, the Supreme Court distinguished the liability of a seller of "articles of free commerce" from that of a seller of restricted goods. Direct Sales, 319 U.S. at 710. The jury must be made aware that the nature of the goods is relevant to its determination of whether Harris had the knowledge and intent necessary to join a conspiracy with TCNISO customers. Id. In those cases, the Supreme Court held that the restricted nature of a product could tend to show that the seller had the knowledge and intent necessary to join a conspiracy with buyers. Id. This holding, combined with the holding in Falcone, clearly indicates that such inferences regarding knowledge and intent cannot be drawn from the nature of an unrestricted product.

[2] Were this statement not true, manufacturers and distributers of common products, including guns, alcohol, chef's knives, and hammers, could and would face criminal charges based solely on the known capabilities of those products to cause harm. However, even civil liability for such individuals is rare. See, e.g., Perkins v. F.I.E. Corp., 762 F.2d 1250, 1265 n.43 (5th Cir. 1985) ("The marketing of a handgun is not dangerous in and of itself, and when injury occurs, it is not the direct result of the sale itself, but rather the result of actions taken by a third party."). Allowing culpability to rest on capability alone would also have the effect of eliding important elements, including knowledge and intent.

[3] Numerous courts have recognized that product capability alone cannot support criminal liability for a seller. In Direct Sales, the Supreme Court noted that "[a]ll articles of commerce may be put to illegal ends" and warned that "to establish the intent [to join a conspiracy], the evidence of knowledge must be clear, not equivocal," because "charges of conspiracy are not to be made out by piling inference upon inference, thus fashioning what, in [Falcone], was called a dragnet to draw in all substantive crimes." Direct Sales, 319 U.S. at 710-11. As discussed in Harris's motion to dismiss, it has long been accepted law that product capability does not give rise to even civil liability for a seller based on the conduct of product users. George A. Nation, Respondeat Manufacturer, 60 Baylor L. Rev. 155, 157-58 (2008) ("Usually the criminal use of a product is deemed to be a supervening, intervening event that eliminates any responsibility on the part of the manufacturer."); Oliver Wendell Holmes, Privilege, Malice, and Intent, 8 Harv. L. Rev. 1, 10 (1894) (stating that usually vicarious liability for a seller does not exist because "every one has a right to rely upon his fellow-men acting lawfully, and, therefore, is not answerable for

3. Uncapping a modem to obtain faster service than you have paid for is not illegal; it is a violation of the ISP's terms of service.[4]

4. A product supplier who does not communicate with users beyond the mere sale of the item is not liable for the conduct of those purchasers.[5]

5. The seller of a product that is legal to sell is not liable for the criminal use of that product by a user even if the seller knows of the use.[6]

6. Proof that Harris knew that TCNISO modems could be used to obtain free internet is not sufficient to establish his guilt; the government must prove that Harris knew that a given user was planning to get free internet from a certain ISP and that Harris intended to help that user to obtain free internet access. Indifference to the

---

himself acting upon the assumption that they will do so, however improbable it may be" (emphasis added)). Nor is suspicion of criminal activity alone sufficient to support a fraud conviction. See United States v. Loder, 23 F.3d 586, 591 (1st Cir. 1994) (in case where defendant's alleged role in mail fraud was helping to dismantle a car, court held that "Although he need not be aware of all the details of the mail fraud, a general suspicion on Loder's part that his participation in dismantling the Caprice was 'for some nefarious purpose' is not enough to make him guilty of aiding and abetting mail fraud.").

[4] Even the intentional breach of a terms of service agreement cannot be the basis for criminal liability. See United States v. Drew, 259 F.R.D. 449, 466-67 (C.D. Cal. 2009) (holding that intentional violation of MySpace's terms of service could not form basis for conviction–by misrepresenting the identify of the user–under 18 U.S.C. § 1030(a)(2)(C)).

[5] Making a seller liable based solely on shipping the product, without further communication, is tantamount to imposing liability based solely on product capability. Without communication or some link beyond the existence of the product itself, there can be no meeting of the minds, no knowledge of the purchaser's plans, and no intent to further those plans.

[6] "[O]ne does not become a party to a conspiracy by aiding and abetting it, through sales of supplies or otherwise, unless he knows of the conspiracy; and the inference of such knowledge cannot be drawn merely from knowledge the buyer will use the goods illegally." Direct Sales Co. v. United States, 319 U.S. 703, 711 (1943).

users' purpose is not sufficient to establish guilt.[7]

7. The operator of an internet forum is not responsible for the content of posts on that forum and is not assumed to know the contents of those posts.[8]

8. There is no law prohibiting the creation or use of devices, called "sniffers," which can be used to obtain data sent between computers. Major corporations such as Google routinely use sniffers to gather information about their customers. There is no law prohibiting the use of a sniffer to harvest MAC addresses or configuration files, and there is no law prohibiting sharing these addresses or files

---

[7] This instruction is drawn from the Supreme Court opinion in Direct Sales: "[O]ne does not become a party to a conspiracy by aiding and abetting it, through sales of supplies or otherwise, unless he knows of the conspiracy; and the inference of such knowledge cannot be drawn merely from knowledge the buyer will use the goods illegally." Additionally, in order to be secondarily liable for a crime, one must intend the end of that crime. United States v. Peoni, 100 F.2d 401, 401-02 (2nd Cir. 1938) (holding that accessorial liability requires that the defendant "in some sort associate himself with the venture, that he participate in it as in something that he wishes to bring about, that he seek by his action to make it succeed."); see also United States v. Medina-Roman, 376 F.3d 1, 3 (1st Cir. 2004). Here, the targeted, allegedly criminal primary conduct at the base of this indictment is obtaining free or faster internet access. Accordingly, in order to be secondarily liable for someone obtaining free or faster internet access, Harris must have known that the user was planning that conduct and he must have intended to assist them in reaching that end. See United States v. Urciuoli, 513 F.3d 290, 300 (1st Cir. 2008) (holding that in fraud cases, government must prove that defendant willfully participated "in [the] scheme with knowledge of its fraudulent nature and with intent that these illicit objectives be achieved" (internal quotation marks omitted)).

[8] This instruction derives from 47 U.S.C. § 230(c)(1), which states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." See Universal Communication Systems, Inc. v. Lycos, Inc., 478 F.3d 413, 415 (1st Cir. 2007) ("Congress has granted broad immunity to entities . . . that facilitate the speech of others on the Internet."). Nor does Harris become liable for the speech of others if he knows that it conveys unlawful information: "notice of the unlawful nature of the information provided is not enough to make it the service provider's own speech." Id. at 420. An instruction along these lines is critical, because the government seeks to string together a conspiracy involving all potential actors at all potential times against all victims using the content of the forum, protected speech for which Harris is not liable.

with other individuals.[9]

10. Proof that Harris sold an item, or that an individual purchased it from him, is insufficient to establish that Harris conspired with or aided and abetted these product customers.[10]

11. An individual cannot aid and abet or conspire in a crime that he is not aware of.[11]

III. CONSPIRACY ISSUES

The government has stated its intention to prove a single, hub-and-spoke conspiracy encompassing Harris, Isabella Lindquist, Craig Phillips, the four named Massachusetts users, and unspecified others. In its proposed instructions the government has conceded that it must prove *this* conspiracy, as charged in the Superseding Indictment, in order to obtain a conviction.

---

[9] See, e.g., Motion to Dismiss Plaintiff's Consolidated Class Action Complaint, In re Google Inc. Street View Electronics Communications Litigation, No. 5:10-md-02184 JW at 3 (9th Cir. Mar. 21, 2011). Companies including Google, Microsoft, and Apple use this information to help device users pinpoint their location. Id.; see also Leena Rao, Microsoft Taps Navizon to Power Mobile Geolocation, Washington Post, Mar. 2, 2010, available at http://www.washingtonpost.com/wp-dyn/content/article/2010/03/02/AR2010030201828.html. Discovery reveals that while investigating Hanshaw, the FBI used a program called Network Stumbler to detect wireless networks in a given area. See Discovery, Bates No. Harris1411-12, Harris1517-18. The FBI used this program on a normal laptop computer running a publicly available Windows operating system. This program detected wireless networks and revealed the MAC addresses of the associated modems to the FBI agent running the program. It appears that the FBI did not have a warrant authorizing the use of this program to reveal MAC addresses and was not otherwise concerned about the legality of this sniffing.

[10] This is black letter conspiracy law. United States v. Santiago, 83 F.3d 20, 23-24 (1st Cir. 1996) ("[A] buyer-seller relationship, simpliciter, is an insufficient predicate for finding that the buyer and seller are guilty as coconspirators."); see also United States v. Moran, 984 F.2d 1299, 1302-03 (1st Cir. 1993); United States v. Gee, 226 F.3d 885, 895 (7th Cir. 2000) (noting, in case involving defendants accused of selling modules that enabled users to receive free television service, that "mere buyer-seller relationship" is not a conspiracy).

[11] This instruction is derived from black letter law as well as basic logic. One cannot intend to assist in a crime unless he knows that a crime is intended or occurring.

A. General Principles

To establish a conspiracy, the government must prove that Harris "knowingly and voluntarily agreed with others to commit a particular crime.'" United States v. Rivera-Rodriguez, 617 F.3d 581, 596 (1st Cir. 2010) (emphasis added) (quoting United States v. Rivera Calderon, 578 F.3d 78, 88-89 (1st Cir. 2009)). The government must prove that Harris knew and intended the specific criminal objective at the heart of the conspiracy. Rivera-Rodriguez, 617 F.3d at 596; see also United States v. United States Gypsum Co., 438 U.S. 422, 443 n.20 (1978); United States v. Ortiz, 447 F.3d 28, 32-33 (1st Cir. 2006). The government must establish that Harris had the "intent to agree and intent to commit the substantive offense." Id. (quoting United States v. Bristol-Martir, 570 F.3d 29, 39 (1st Cir. 2009)). In this case, the substantive offense/criminal objective charged is wire fraud based on users' attempts to utilize TCNISO products to get free or faster internet access. Accordingly, in order to prove the charged conspiracy, the government must prove that Harris agreed with product users to commit wire fraud through the users' attempts to get free internet and that he intended to commit wire fraud through their attempts to do so. As charged, the "particular" crime underlying this conspiracy occurred when each user either obtained a TCNISO product or used the product to get free internet. Therefore, the government must prove that Harris knew that each user was going to use the product to get free internet, and that he intended to join in each individual's efforts to obtain free internet access.

B. Continuity of Offense

The government's case presumes that buying an item and later using the item merge into a single offense. Its case rests on the premise that once an individual obtained a product from

Harris, Harris and that individual were engaged in a conspiracy that continued each time the individual used the product. There are no time limits implicit in the government's charge. However, "[a] conspiracy does not continue indefinitely simply because the fruits of the conspiratorial objective continue into the future." United States v. Colon-Munoz, 192 F.3d 210, 228 (1st Cir. 1999). In United States v. Doherty, 867 F.2d 47 (1st Cir. 1989), the government charged a conspiracy to commit mail fraud, masterminded by one individual, "to steal copies of examinations and sell them to policemen seeking promotions." Id. at 51. While considering the statute of limitations, the Court concluded that receiving and using the stolen exam, the object of the conspiracy, was separate from the act of continuing to receive a salary inflated by the promotion obtained through the use of the stolen exam. Id. at 60-62.

> [W]her receiving the payoff merely consists of a lengthy, indefinite series of ordinary, typically noncriminal unilateral actions, such as receiving salary payments, and there is no evidence that any concerted activity posing the special societal dangers of conspiracy is still taking place, we do not see how one can reasonably say that the conspiracy continues. Rather, in these latter circumstances, one would ordinarily view the receipt of payments merely as the "result" of the conspiracy.

Id. at 61. The Supreme Court has similarly held: "Though the result of a conspiracy may be continuing, the conspiracy itself does not thereby become a continuing one. Continuity of action to produce the unlawful result, or . . . continuous co-operation of the conspirators to keep it up is necessary. A conspiracy is a partnership in crime." Fiswick v. United States, 329 U.S. 211, 216 (1946) (citations and quotation marks omitted); see also United States v. Goldberg, 105 F.3d 770, 774 (1st Cir. 1997) ("[M]ere collateral effects of jointly agreed-to activity, even if generally foreseeable, are not mechanically to be treated as an object of the conspiracy.").

These rulings highlight the fact that a conspiracy does not necessarily encompass its

results. Here, the government has lumped together two distinct types of actions; the purchase of a device that it alleges is inherently nefarious, and the results that flow from that sale, results that the government would say are inevitable. However, as these cases illustrate, the results of a conspiracy cannot be grouped into a conspiracy as part of the crime.

C. Communication with Users

Additionally, in order to prove the hub and spoke conspiracy as charged, the government must prove that Harris knew of each alleged user and of his or her intentions. The government asserts that the defendant need not communicate with his or her co-conspirators. Gov't Tr. Br. at 17. In support of this statement, the government cites United States v. Mena-Robles, 4 F.3d 1026, 1033 (1st Cir. 1993). However, a careful examination of this case reveals that the Court's ruling was more limited than the government suggests: "[A] single conspiracy may exist where there has been no direct contact among some of the participants." Id. at 1033 (emphasis added). Mena-Robles then cites United States v. Giry, a case that explains the typical scenario in which communication between co-conspirators is not necessary. Id. In United States v. Giry, 818 F.2d 120, 127 (1st Cir. 1987), the Court noted that the typical "scheme to manufacture and distribute a large quantity of illicit drugs involves a great many discrete steps and includes a large number of people, most of whom know few of the other participants in the scheme." The Court explained that this type of arrangement is viewed as a single, "chain" conspiracy because "[e]ach participant's financial gain depends upon the successful accomplishment of all the illegal links in the chain, from manufacturing, transporting and wholesaling the drugs down to each retail sale on the street." Id. One can assume that in such a chain conspiracy, each link in the chain has at least communicated with the link directly above and below itself, so that there is an established

flow of information and directions from top to bottom. The top level may only know and direct the second level, but it knows what it has told the second level to do, and therefore knows what the second level will set in motion down the chain. Similarly, the bottom level may only speak to one level above itself, but it knows that when it requests and pays for drugs, those drugs are forthcoming.

That level of interdependence and that type of internal communication cannot be assumed in the hub and spoke conspiracy charged here. See United States v. Pappathanasi, 383 F.Supp.2d 289, 193-94 (noting that most co-conspirators never communicated with defendants in alleged hub and spoke conspiracy). Accordingly, the government must prove actual communication and actual interdependence. Unlike in a chain conspiracy, it cannot be inferred from the structure of the alleged scheme that Harris knew of and intended the boundless conspiracy charged. The case charged is not like a drug ring or a food chain where each level depends on the other, interaction notwithstanding, in a perpetual cycle. Harris did not gain anything specific from a particular users's success, and a particular user did not depend on Harris's continued work. Instead, the government must prove that Harris knew about each alleged conspirator and that he intended to join in each conspirator's actions and to further their attempts to get free internet access. Therefore, the government must prove that Harris communicated with the alleged product users and that he was aware of their objectives and intended to help them to get free internet access if they so desired.

D. Buyer-Seller

A similar result is dictated by the Supreme Court precedent related to buyer-seller relationships and conspiracies. "[A] buyer-seller relationship, simpliciter, is an insufficient

predicate for finding that the buyer and seller are guilty as coconspirators." United States v. Santiago, 83 F.3d 20, 23-24 (1st Cir. 1996)(emphasis in original); see also United States v. Moran, 984 F.2d 1299, 1302-03 (1st Cir. 1993); United States v. Gee, 226 F.3d 885, 895 (7th Cir. 2000) (noting, in case involving defendants accused of selling modules that could enable cable converter boxes to receive free television service, that a "mere buyer-seller relationship" is not a conspiracy). Even in narcotics cases, courts will not infer a conspiracy based on a one-time sale or multiple "casual" sales where there is no indication that the seller is committed to the buyer. See e.g. Moran, 984 at 1302-03; United States v. Izzi, 613 F.2d 1205, 1210 (1st Cir. 1980); United States v. Thomas, 284, F.3d 746, 751-54 (7th Cir. 2002); United States v. Gore, 154 F.3d 34, 40-41 (2d. Cir. 1998); United States v. Mancari, 875 F.2d 103, 105 (7th Cir. 1989).

In order to prove that the alleged buyer-seller relationship was a conspiracy, the government must prove that Harris had "clear, not equivocal" knowledge of the conspiracy and intended to join it. Direct Sales Co. v. United States, 319, U.S. 703, 711 (1943). The "inference of such knowledge [of a conspiracy] cannot be drawn merely from knowledge the buyer will use the goods illegally." Id. at 709; see also United States v. Ocampo, 964 F.2d 80, 82 (1st Cir. 1992) (finding that "a fair inference that defendant knew what was going on" does not "establish intent to conspire."); Pappathanasi, 383 F.Supp.2d at 291 ("The mere collateral effects of jointly agreed-to activity, even if generally foreseeable, are not necessarily an object of the conspiracy."); Goldberg, 105 F.3d at 774. Nor does "the act of supplying itself" demonstrate "an agreement or concert of action between the buyer and the seller amounting to conspiracy." Direct Sales, 319 U.S. at 709. To prove a conspiracy, the government must show that, "by the sale, [the seller] intends to further, promote, and cooperate in [the buyer's intended illegal use]."

Id. at 711. "[N]ot every instance of sale of restricted goods, harmful as are opiates, in which the seller knows the buyer intends to use them unlawfully, will support a charge of conspiracy." Id. at 712. "[I]ndifference to the buyer's illegal purpose" is insufficient to prove a conspiracy. Id. at 712, n.8.

Applying these precedents to the facts of this case leads to the conclusion that the government must prove that each alleged user planned to use TCNISO products to obtain free internet, that Harris knew this, and that Harris intended to help each user to obtain free internet. It is not enough for the government to show that Harris intended to help everyone in the world to get free internet access for all time; the government must show that Harris knew that *these* users intended to use TCNISO products to get free internet access and that Harris intended to help *these* individuals to get free internet access.

E. Single Conspiracy

A conspiracy is measured by the scope of the agreement underlying the conspiracy, and one conspiracy can include more than one substantive offense. Braverman v. United States, 317 U.S. 49, 53-54 (1942). "A single agreement to commit several crimes constitutes one conspiracy. By the same reasoning, multiple agreements to commit separate crimes constitute multiple conspiracies." United States v. Broce, 488 U.S. 563, 570-71 (1989). The existence of a single conspiracy is decided based on the "totality of the circumstances," with a focus on the "existence of a common goal, evidence of interdependence among the participants, and the degree to which their roles overlap." United States v. Fenton, 367 F.3d 14, 19 (1st Cir. 2004).

To establish a common goal, the government must prove an "overall objective to be achieved by multiple actions." United States v. Chandler, 388 F.3d 796, 811 (11th Cir. 2004). In

its trial brief, the government states that: "Here, the common goal was for users to obtain free or faster internet service from ISPs by disguising themselves as legitimate, paying subscribers. In turn, the conspirators' goal was to profit financially–the users by avoiding subscriber fees and Harris by earning sales revenues." Gov't Tr. Br. at 21. These statements plainly reveal the fact that no common goal exists in this case. According to the government, Harris's motive was to sell a variety of modems and software and to make money. Also per the government, each of the alleged user's motive was to get free internet access and to save money. Clearly these divergent motives cannot be considered a common goal. Not only are these interests different, they are potentially in conflict; Harris's desire to make money is plainly incompatible with the desire of others to save money. Additionally, as in Pappathanasi, the users were not dependent on one another, and each decided to engage in illegal conduct of his or her own accord. 383 F.Supp.2d at 296-97.

The government has stated that it intends to prove that there was a single conspiracy because an internet forum on the TCNISO website served as a rim to connect all of the spokes. This forum is the sole evidence that the government has proffered to connect the spokes, and the government's case that there is a single conspiracy rests entirely on the existence of the forum. But chats on a forum are not admissible, see pp.23-26, infra, and forum moderators are not liable for forum content.

The owner or host of a forum is legally immune from responsibility for material that is posted on the forum: "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1); see also Universal Communication Systems, Inc. v. Lycos, Inc., 478 F.3d

413, 415 (1st Cir. 2007) ("Congress has granted broad immunity to entities . . . that facilitate the speech of others on the Internet."). Nor does a forum provider become liable for the speech of others if he knows that it conveys unlawful information: "notice of the unlawful nature of the information provided is not enough to make it the service provider's own speech." Id. at 420. Not only is Harris shielded from liability for the content of the forum, the posters on the forum were completely anonymous and posted under screen names of their own devising. Given this anonymity, the government cannot prove that the content of the forum is admissible co-conspirator hearsay under United States v. Petrozziello, 548 F.2d 20, 23 (1st Cir. 1977). See also United States v. Sepulveda, 15 F.3d 1161, 1180 (1st Cir. 1993). The sole evidence of the requisite "rim" is barred by the immunity statute and the hearsay rules.

IV. WIRE FRAUD PROOF

A. Principal

To sustain a wire fraud conviction based on the theory that Harris acted as a principal, the government must prove that Harris knowingly and willfully devised a scheme or artifice to defraud, had the specific intent to deprive another of something of value or to obtain something of value, and used interstate wire communications in furtherance of this scheme. 18 U.S.C. § 1343; United States v. Woodward, 149 F.2d 46, 63 (1st Cir. 1998). With respect to the use of the interstate wire, the government must prove that Harris either made the charged transmission or caused the charged transmission to be made. The government asserts that each alleged user was involved in two types of wire fraud: wire fraud based on the interstate wire transmission that occurred when the user bought or downloaded a TCNISO product, and wire fraud based on the interstate wire transmission that occurred when the user accessed the internet without paying

using TCNISO products. Therefore, in order to prove that Harris acted as a principal in these charges, the government must prove that Harris either accessed the internet himself (via the users' computers and TCNISO products) on the charged occasions, or caused the users to access the internet on the charged dates.

Additionally, to convict Harris as a principal, the government must prove that Harris devised a scheme to defraud and specifically intended to obtain something of value or to deprive another of value. The government alleges that the scheme that was devised was to obtain internet access without paying. Outside of the conspiracy arena, the government must make specific showings regarding the discretely charged wire frauds. Accordingly, for each count of wire fraud, the government must prove that Harris devised a scheme to defraud the ISP charged, and that in so doing he specifically intended to deprive that ISP of something of value or that he specifically intended to obtain something of value as a result of the scheme to defraud that ISP. The government would also have to prove that the charged communication was made in furtherance of the scheme to defraud that ISP.

The government states that it does not have to prove that Harris personally benefitted from the wire fraud to obtain a conviction. The cases cited by the government do not stand for the proposition that personal benefit is not required to establish wire fraud. The cases cited by the government stand for the proposition that, in an honest services fraud case, the government need not show that anyone benefitted from the scheme so long as it can prove that the government was deprived of the honest services due it. See United States v. Silvano, 812 F.2d 754, 758-62 (1st Cir. 1987); United States v. Vila, 2009 WL 79189; 2009 U.S. Dist. LEXIS 2729 (D.P.R.). Harris is not charged with honest services fraud, and therefore the deprivation of his

honest services cannot stand in for proof that he benefitted from the alleged scheme to defraud. Instead, to convict Harris as a principal, the government must prove that he intended to either deprive someone else of something of value or to obtain something of value himself as a result of the scheme to defraud. The government may prove one of two things in connection with each wire fraud count: 1) that Harris deprived an ISP of something of value through his scheme to defraud ISPs, and that the alleged communication was made or caused by Harris in service of this scheme; 2) that Harris obtained something of value through his scheme to defraud ISPs, and that the alleged communication was made or caused by Harris in service of this scheme.

B. Aiding and Abetting

To establish that Harris aided and abetted wire fraud by product users, the government must prove that the alleged users committed wire fraud as charged and that Harris willfully associated himself with that wire fraud and willfully participated in it with an intent to realize the charged offense.

Accessorial liability requires that the alleged accessory "in some sort associate himself with the venture, that he participate in it as in something that he wishes to bring about, that he seek by his action to make it succeed." United States v. Peoni, 100 F.2d 401, 401-02 (2nd Cir. 1938); see also United States v. Medina-Roman, 376 F.3d 1, 3 (1st Cir. 2004). To prove accomplice liability, the government must establish that the defendant had the same mens rea as the principal, in this case, specific intent to achieve the illicit objective. See United States v. Serrano, 870 F.2d 1, 6 (1st Cir. 1989). Therefore, the government must first prove that the alleged users committed wire fraud, that is, that each one devised a scheme to defraud (per the government, getting internet access without paying), that each user intended to obtain something

of value or to deprive someone else of something of value (alleged to be unpaid access to the internet), and that each user made an interstate wire transmission as charged in the superseding indictment. Then the government must prove that Harris knew about each user's scheme and intention and that he purposely joined in the venture of each user with the intent to help that user realize his own wire fraud scheme. Because each user allegedly had a scheme to defraud his or her own ISP, the government must prove that Harris had the same specific intent to defraud each ISP. Such shared knowledge and intent cannot arise without some communication, or at least some knowledge on the part of Harris regarding each user and his or her personal objectives.

It is not enough to prove that Harris may have had some knowledge that something underhanded was occurring; the government must prove that Harris willfully participated "in [the] scheme with knowledge of its fraudulent nature and with intent that these illicit objectives be achieved." United States v. Urciuoli, 513 F.3d 290, 300 (1st Cir. 2008) (internal quotation marks omitted). In a mail fraud case charging the defendant with aiding the fraud by helping to dismantle a brand new car, the First Circuit explained:

> In order to sustain a conviction in the instant case, the government must show that the defendant, Paul Loder, consciously shared in the specific criminal intent of the principals, the Morrisons, to commit mail fraud. In other words, the government must present evidence that would allow a rational trier of fact to conclude that Loder had knowledge that he was furthering mail fraud. Although he need not be aware of all the details of the mail fraud, a general suspicion on Loder's part that his participation in dismantling the Caprice was "for some nefarious purpose" is not enough to make him guilty of aiding and abetting mail fraud.

United States v. Loder, 23 F.3d 586, 591 (1st Cir. 1994) (citing United States v. Barclay, 560 F.2d 812 (7th Cir. 1977) (reversing conviction for bank fraud and abetting bank fraud because trial judge's instructions permitted convicted without finding that defendant knew that the

principal was going to make a false entry with the specific intent to defraud the bank and without finding that defendant shared the principal's specific intent to defraud the bank).

V. RELEVANCE AND LAY OPINION ISSUES

The government plans to introduce a large amount of evidence that should be excluded as irrelevant and unduly prejudicial under the Rules of Evidence.

A. Craig Phillips's Testimony

The government proposes that Phillips will testify about the day-to-day operations of TCNISO and the products that TCNISO offered. This testimony is irrelevant, because Phillips only worked for TCNISO until 2007. All three of the customers who allegedly purchased items from TCNISO did so after 2007. Accordingly, anything Phillips knows about how products were shipped, how the forum was moderated, how product updates were designed, or how Harris behaved have no relevance to the charges, as Phillips has no personal knowledge about how the company was run at the time that the charged purchases occurred. Nor is there any evidence that Phillips has the expertise necessary to provide expert testimony explaining how the products worked. Accordingly, this testimony should be excluded under Rules 402, 602, and 702.

Phillips is also expected to testify that Harris showed him how to use TCNISO products to get free or enhanced internet and that he saw Harris use the products to do so. This evidence is irrelevant and unduly prejudicial other acts evidence under Rules 402 and 404(b). The government has not charged Harris with his own use of TCNISO products, and this evidence is not relevant to the case at hand. Instead, this evidence, particularly testimony that he needed free internet to download music and videos more quickly, would serve only to show propensity. Ample evidence, including Harris's book, will show that Harris knew that TCNISO products

could be used to obtain free or uncapped internet. The critical issues in this case involve whether Harris had the requisite knowledge and intent to help a given user get free internet from a given ISP. Evidence that Harris knew something could happen is not evidence that he knew that it would happen or that he intended to help other people make it happen. See Pappathanasi, 383 F.Supp.2d at 291-92. Evidence that Harris himself used the products to obtain free internet does not shed any light on this contested issue.

This evidence must be excluded under Rule 404(b) because "[i]t involves an inference of propensity as 'a necessary link in the inferential chain.'" United States v. Varoudakis, 233 F.3d 113, 120 (1st Cir. 2000). In Varoudakis, the First Circuit held that evidence that the defendant had committed a prior arson was inadmissable because it was offered to show propensity–that because the defendant had committed a prior arson because of financial difficulties, it was "more likely that he committed the [charged] arson in response to financial stress." Id. The proffered evidence regarding Harris's use of TCNISO products serves the same purpose; it would cause the jury to infer that because Harris intended to get and got free or enhanced internet access using TCNISO products, he intended for others to obtain the same benefit using the same products. Rule 404(b) prohibits the use of prior bad acts to show propensity in this way, and testimony regarding Harris's use of TCNISO products should be excluded.

The government states that Phillips will testify that TCNISO was created to help people get free internet, that he intended to help people do so, and that he thought his conduct was illegal. Phillips will also testify that these products had no other use and that Harris was paranoid and had a personal vendetta against the cable companies. Any testimony from Phillips about what he thought Harris thought, felt, or knew is inadmissible opinion testimony outside of his

personal knowledge. Fed. R. Evid. 602. Phillips has not been offered as an expert witness, and nothing in his background indicates that he is qualified to opine about design choices that were made or other marketable uses of the products. Accordingly, any testimony along these lines should be excluded under Rules 602 and 702.

Finally, Phillips will testify that Harris told him that they were going to get rich from TCNISO. This testimony is irrelevant and should be excluded under Rule 402. This testimony does not tend to prove that Harris benefitted from the alleged scheme because: 1) it does not prove that Harris made money from selling altered modems, and 2) it does not establish that Harris benefitted from his customers. attempts to obtain free internet.

For reasons that will be discussed below, Harris also objects to the introduction of chat transcripts through this witness.

B. Isabella Lindquist's Testimony

Harris objects to the introduction of some of Lindquist's testimony on relevance grounds. Like Phillips, the government expects Lindquist to testify about how TCNISO was run. Lindquist will testify about the company's operations between 2002 and 2008. As with Phillips, this testimony is irrelevant because the named users who purchased products from TCNISO did so in 2008 and 2009. Therefore, any information Lindquist has about how the company was run does not shed any light on how it was run at the time the purchases at issue were made. Additionally, Lindquist has never met Harris in person, never saw the TCNISO operations in person, and has limited personal knowledge about how things were run at any time. Lindquist is also expected to testify that Harris told her that they were going to make lots of money. Harris objects to this testimony, because it does not show that Harris made money selling modems or

tend to show that Harris benefitted from users choosing to use his product to obtain free internet.

Lindquist is also expected to testify about what Harris told her about the contents of the forum. As discussed below, Harris objects to any introduction of the forum posts or description of their content. He also objects to the introduction of any chat transcripts through this witness.

Finally, Lindquist is expected to testify about her online conversations with Nathan Hanshaw. Harris objects to this testimony on the hearsay grounds described below. Harris also objects to Lindquist's testimony that Harris communicated with Hanshaw, because she does not have personal knowledge regarding any such communications. Fed. R. Evid. 602.

C. Massachusetts Users

As discussed below, Harris objects to the introduction of any chat communications or forum posts, or testimony about them, through these witnesses.

D. ISP Employee

The government proposes to have Benjamin Brodfeuhrer testify about the costs imposed on ISPs by TCNISO products and the financial injury suffered by Charter. Harris argues that this testimony is irrelevant and would only serve to distract the jury from the issues at hand.

E. Law Enforcement Agents

The government plans to have Special Agent Timothy Russell testify about and introduce content from the TCNISO forums. For reasons that will be discussed below, Harris objects to this testimony and content as hearsay.

The government intends to have Special Agent Jason Ryan testify about TCNISO's financial records, including how much money came in and how much was paid to employees. Harris asserts that this testimony is irrelevant because it does not tend to show that Harris

benefitted from the actions of users who were able to obtain free internet.

VI. HEARSAY OBJECTIONS AND AUTHENTICATION PROBLEMS

A. Modem Employee

The government expects that Christopher Kohler, a Motorola employee, will testify that he received numerous complaints from ISPs about TCNISO products. His testimony about what he was told is hearsay to which no exception applies that must be excluded. Fed. R. Evid. 801.

B. TCNISO Website Forum Posts

The government intends to introduce testimony about the content of the TCNISO user forum, as well as some actual posts from the forum. Harris objects to the introduction of such testimony and posts, as he is statutorily immune from responsibility for these posts and, in any event, they are hearsay for which no exception exists.

In the interest of encouraging and protecting free speech, Congress has given the owner or host of a forum statutory protection from legal responsibility for content that others post on the forum: "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1). The First Circuit has recognized this protection and its importance. Universal Communication Systems, Inc. v. Lycos, Inc., 478 F.3d 413, 415 (1st Cir. 2007) ("Congress has granted broad immunity to entities . . . that facilitate the speech of others on the Internet."). This protection is strong enough that a forum provider does not become liable for the speech of others even if he knows that it conveys unlawful information: "notice of the unlawful nature of the information provided is not enough to make it the service provider's own speech." Id. at 420.

Here, the government seeks to introduce the content of a forum as though it is attributable

to Harris, as though he was aware of all of the content and even caused others to use the forum. The forum is the sole evidence that the government has offered to show that the users of TCNISO products were connected to one another in a single conspiracy, and thus the forum is a necessary component of the government's theory of criminal liability. Plainly, using content that was posted on a public forum by anonymous users to form the basis for criminal liability, runs counter to these statutory commands. This statute dictates that Harris cannot be presumed to be familiar with the content on the TCNISO forum and that the criminal liability cannot derive from the existence of the forum or its content.

Not only are the forum posts an inappropriate basis for criminal liability, they are hearsay for which no exception exists. The government argues that these posts are admissible because they are verbal acts, not statements. However, the words that users typed on the forums are not like words by contracting parties; they have no independent legal significance. 5 Weinstein's Federal Evidence § 801.11(3). The First Circuit case that the government cites to support its proposition that such utterances are admissible did not consider whether the utterances at issue were properly admitted as non-hearsay verbal acts, because the Court found that any error was harmless. United States v. Diaz, 597 F.3d 56, 65 (1st Cir. 2010).

Next, the government asserts that the forum posts are admissible because they are not being introduced for the truth of the matter asserted, but to show their effect on Harris. There is no evidence that Harris read any particular post and that the ones the government seeks to introduce had any effect on him. This argument is an attempt to avoid the co-conspirator hearsay rule. Rule 801 defines statement as an oral or written assertion. Fed. R. Evid. 801(a). It defines hearsay as a particular type of statement. Fed. R. Evid. 801(c). It also creates specific rules for

when certain types of statements are not considered hearsay. Fed. R. Evid. 801(d). One of these targeted rules explains that a statement under Rule 801(a) is not hearsay if it is made by "a coconspirator of a party during the course and in furtherance of the conspiracy." Fed. R. Evid. 801(d)(2)(E). The government alleges that the individuals who wrote the forum posts were co-conspirators with Harris, and these statements are admissibly only if they meet the rule contained in Fed. R. Evid. 801(d)(2)(E).

These posts are not admissible under Rule 801(d)(2)(E). This exception is a narrow one that has been criticized by courts, including the First Circuit. United States v. Goldberg, 105 F.3d 770, 775 (1st Cir. 1997) ("Frankly, the underlying co-conspirator exception to the hearsay rule makes little sense as a matter of evidence policy. No special guarantee of reliability attends such statements, save to the extent that they resemble declarations against interest. The exception derives from agency law, an analogy that is useful in some contexts but (as the Advisory Committee noted) is 'at best a fiction' here. The most that can be said is that the co-conspirator exception to hearsay is of long standing and makes a difficult-to-detect crime easier to prove."). "To invoke the exception, a party who wants to introduce a particular statement must show by a preponderance of the evidence that a conspiracy embracing both the declarant and the defendant existed, and that the declarant uttered the statement during and in furtherance of the conspiracy." United States v. Sepulveda, 15 F.3d 1161, 1180 (1st Cir. 1993); United States v. Petrozziello, 548 F.2d 20, 23 (1st Cir. 1977). "The contents of the statement shall be considered but are not alone sufficient to establish . . . the existence of the conspiracy and the participation therein of the declarant and the party against whom the statement is offered . . . ." Fed. R. Evid. 801(d)(2)(E). This rule permits the trial judge to determine, before trial,

whether or not a conspiracy existed. See Giles v. California, 554 U.S. 353, 374 (2008) ("A judge may determine the existence of a conspiracy in order to make incriminating statements of co-conspirators admissible against the defendant under Federal Rule of Evidence 801(d)(2)(E).").

There is no evidence apart from the content of these posts to show that there was a conspiracy between the declarant and Harris and that the statements were made in furtherance of that conspiracy. As Harris has argued before, the government has not sufficiently alleged a conspiracy in this case, because a buyer-seller relationship does not make a conspiracy, even when the seller knows of a potential illicit use of the product sold. Additionally, the forum posters have not been identified, and aside from their statements, there is no evidence that they used TCNISO products for any purpose. See Sepulveda, 15 F.3d at 1181 (finding that statements should not have been admitted under coconspirator hearsay exception where there was no evidence beyond the statements to show that the unidentified declarants were part of the charged conspiracy). Evidence that these individuals purchased TCNISO products is not evidence that they bought the products to obtain free or faster internet, or that they succeeded in doing so. It is only their statements that provide any hint of their purposes or actual uses.

C. Chat Logs

Harris objects to the admission or discussion of online chat conversations between himself and other individuals as hearsay to which no exception applies. The government has not provided enough evidence for this court to find, to a preponderance, that a conspiracy existed to which Harris and the declarants were parties. See Sepulveda, 15 F.3d at 1180. This concern is particularly strong in connection with the chat conversations between individuals who will not testify and who have not been identified beyond the screen name they chose to use (Mr. T,

Killswitch, Xfactor, Shagy, and MooreR). There is no evidence outside of the content of the chat conversations that these unidentified individuals participated in a conspiracy with Harris and other users to obtain free internet.

The government also seeks to introduce chat conversations between Nathan Hanshaw and an FBI source that occurred during the investigation of Hanshaw. Harris objects to the introduction of these conversations as there is no evidence that either of these individuals, particularly the unknown FBI source, participated in a conspiracy with Harris.

VII. AUTHENTICATION PROBLEMS

The government obtained the chat logs between Harris and other individuals that it seeks to introduce from Phillips, and it intends to introduce these logs through Phillips. When Phillips left TCNISO, he apparently copied files, including logs of chat conversations, from Harris's computer. When Phillips was arrested and charged, he gave these saved files to the government.

Apart from the hearsay issues discussed above, evidence is not admissible unless it can be authenticated. Fed. R. Evid. 901. The government claims that these chat logs are complete and accurate accounts of online conversations between Harris and other individuals. However, the government has not proffered any witness who can authenticate these logs. Phillips does not have knowledge of how the chat logs were saved on Harris's computer, and he does not know whether those logs were altered in any way before he made his copy. Nor is there any witness who can testify to the accuracy of those copies or to the fact that they have not been altered since they were copied. Testifying witnesses may be able to authenticate chats that they had with Harris, to the extent that they remember the content of online conversations they had years ago, but in the case of chats between Harris and non-testifying individuals, the government will not

present any evidence tending to show that those chat logs are accurate and complete records of conversations. Accordingly, the chat logs must be excluded under Rule 901.

RYAN HARRIS
By his attorney,

/s/ Charles P. McGinty

Charles P. McGinty
B.B.O. #333480
Federal Defender Office
51 Sleeper Street
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on August 1, 2011.

/s/ Charles P. McGinty

Charles P. McGinty